Exhibit C

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- -X

UNITED STATES OF AMERICA

    - against -

KEITH RANIERE,

             Defendant.
- -X

DECLARATION

Criminal Docket No. 18-204 (NGG)

EASTERN DISTRICT OF NEW YORK, SS:

        David Loveall II, Senior Computer Scientist with the Federal Bureau of

Investigation ("FBI"), hereby declares under penalty of perjury, pursuant to 28 U.S.C. § 1746:

        1.   I am a Senior Computer Scientist assigned to the Operational

Technology Division (OTD) of the FBI in Quantico, Virginia, where I have worked since

May 2010. I was previously employed as a forensic examiner for the FBI in Kansas City.

As a Senior Computer Scientist of OTD, I advise FBI personnel on issues related to digital

forensics and computer science. I research emerging technologies that may impact FBI

investigations; transition technology solutions from academia, other government agencies,

and the private sector; and develop custom software solutions to address FBI investigative

challenges.

        2.   I was not involved in the investigation or prosecution of United States

v. Keith Raniere, 18-CR-204 (NGG).

        3.   At the request of the United States Attorney's Office in the Eastern

District of New York, I have reviewed a document titled "Summary of Technical Findings"

authored by J. Richard Kiper and dated April 25, 2022 (the "Kiper Report"). I was also

1

provided with access to certain evidence, including a Western Digital Hard Drive (1B16), and a Canon EOS 20D camera (1B15) and CompactFlash (CF) camera card (1B15a).

4.   As set forth below, many of the conclusions set forth in the Kiper Report are misleading or erroneous. The Kiper Report repeatedly ignores plausible explanations for observed phenomena in favor of allegations of tampering.
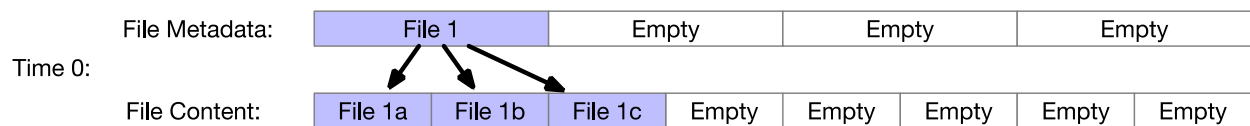
First Finding

5.   Kiper's analysis is faulty with respect to the first finding that "some digital photo files found on the CF card" had properties that "prov[e] manual alteration of the CF Card contents." The Kiper Report states that some of these digital photographs "had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people" and that they "contained thumbnail pictures from another existing set of photos." Kiper's conclusion that this proves that the card's contents must have been intentionally altered is not correct. File Allocation Table ("FAT") file systems routinely produce results like those observed here, under conditions in which files are regularly created and deleted over time, and digital forensic tools are then used to recover the deleted files. This is particularly true if the capacity of the CF card is not sufficient to hold all the photographs taken by the camera, which necessitates the need to delete older photographs to store new ones.
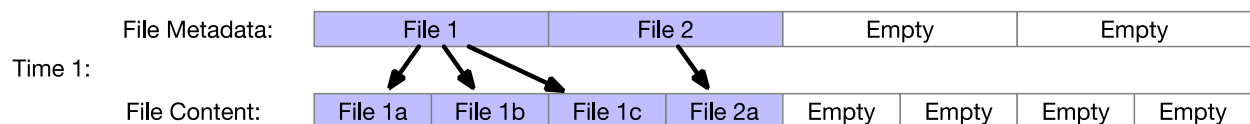
6.   Two points will assist in understanding why this is so. First, metadata (such as filenames and dates) are typically stored in a separate location on media from the actual file content. The location where the filename is stored "points" to the location where the file content is stored, and that is how the file system is able to associate the metadata with

2

the content. Second, when files are deleted, they do not actually disappear from the

underlying media, e.g., the CF card. The file system simply makes available for reuse the

space that those files previously occupied. Unless and until that space is overwritten, those

files remain available for recovery. But when a large file is deleted and a smaller file is

saved in its place, it is possible that some of the larger file can be recovered but not all.
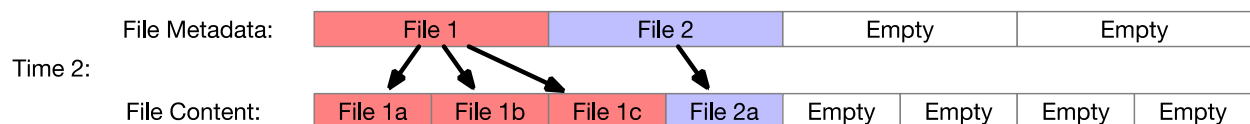
       7.   The phenomenon observed by Kiper reflects the interaction of these

two aspects of the file system, that is, (1) the separation of metadata and content and (2) the

partial recovery of partially-overwritten files. These two aspects can result in metadata from

one file being misattributed to another. For an illustration of this effect, consider a file

system that contains a single file in which the metadata (such as the file name and dates) is in
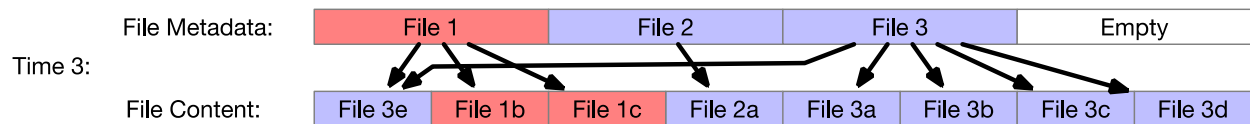
a separate location from the file content:

File Metadata:	File 1		Empty	Empty	Empty

Time 0:

File Content:	File 1a	File 1b	File 1c	Empty	Empty	Empty	Empty	Empty

If a second file is created, it will be given a previously-empty storage location for the file

metadata:

File Metadata:	File 1		File 2		Empty	Empty

Time 1:

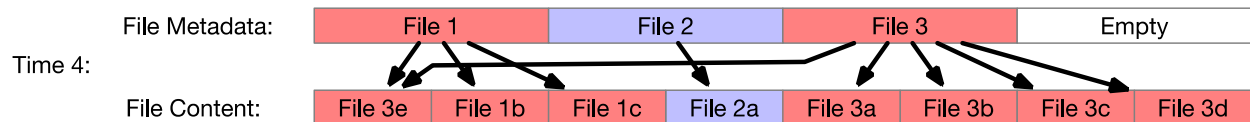| File Content:	File 1a	File 1b	File 1c	File 2a	Empty	Empty	Empty	Empty

If the first file is then deleted, the deleted file metadata and content (marked in red) are

available for use:

File Metadata:	File 1		File 2		Empty	Empty

Time 2:

File Content:	File 1a	File 1b	File 1c	File 2a	Empty	Empty	Empty	Empty

3

If a third file is then created, with a content size that requires five "blocks," the third file will overwrite the content of File 1. In this example, File 1a is then permanently irrevocable and any digital forensic tool would recognize that File 1a is partially overwritten and not recoverable in its original state:

But if File 3 is then deleted, any attempt to recover File 1 or File 3 using an automated digital forensic tool may result in a misattribution of metadata to File 1 in an effort to allow the user of the tool the greatest opportunity to recover usable data:

In this case, File 3 would be recovered successfully but File 1 would contain a portion of File 3.

8.   Therefore, Kiper's claim that the observed phenomenon "prov[es] manual alteration" is simply incorrect.

Second Finding

9.   With respect to the second finding, Kiper claims that "additional files appeared on the FBI's forensic report of the CF Card between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship" between the camera card and the hard drive. This finding is misleading as stated, because the settings used to process and generate the two forensic reports generated on those dates were different. Although both reports used the same processing tool—AccessData Forensic Toolkit 6.3.1.26—there are numerous

configurations and setting options for this tool, which can result in the generation of different

reports. The fact that additional files appeared in one report is a result of the use of different

settings. I have examined the disk images created of 1B15 and 1B15a and determined that

they are identical.

Third Finding

10.   With respect to the third finding, the camera card was accessed on

September 19, 2018. This is consistent with accessing the contents of the card without a

write-blocker.

Fourth Finding

11.   With respect to the fourth finding, Kiper claims that "dates of photos on

the hard drive were altered through manual intervention." In fact, the differences Kiper

identifies is likely attributable to a combination of factors, including the daylight savings

time (DST) shift, contemporaneous manual or automatic changes to device clocks to account

for daylight savings time ending, and a 2006 Microsoft Windows update that introduced

dynamic DST time zones.

12.   In 2006, Microsoft Windows released an update which configured

Windows to use a "dynamic DST" exception for 2006 and 2007. Dynamic DST provides

support for time zones whose boundaries for DST change from year to year. Dynamic time

zones enable easier updating of computers, especially for locates where the yearly DST

boundaries are known in advance.

13.   Where, as here, however, a computer has a system clock set to a pre-

2006 date and applies the DST update, that computer will incorrectly apply the 2007 DST

changes. The Exif data associated with that data, however, is unmodified. The dates of

interest identified in the Kiper Report are between 2005-10-29 05:47:24 AM and 2005-10-30

04:34:20 AM.   The Kiper Report observes that the "Modified" dates of photographs were

"adjusted to be two hours behind" and then, starting with IMG_0138, they were "adjusted to

be exactly the same time as the EXIF dates." Kiper Report at 7.

   14. Kiper's conclusion that "[n]othing outside of human intervention could

account for these changes," is therefore incorrect.

  Fifth Finding

   15. With respect to Kiper's fifth finding, Kiper argues that the fact that the

modification date of a single certain file, IMG_0175, was not updated must be attributable to

manual alteration. Kiper is incorrect, however, as use of the Adobe Photoshop Elements

software does not always result in an updated modification date. For instance, if a user of

Adobe Photoshop Elements clicks on a file and selects "Change to a specified date and time"

for a file and selects "OK" without specifying a new date and time, the file may add its

additional metadata (reflecting that the software was used to "modify" the file), without

actually updating the file's filesystem modify date and time.

  Sixth Finding

   16. With respect to Kiper's sixth finding, it is of course possible to rename

files and folders and any computer user may do so.

  Seventh Finding

   17. Kiper's seventh finding claims notes that certain files on the Western

Digital hard drive have a "created" date of 2003 but have a "last modified" date of October

2005. Kiper acknowledges that when a computer is left out without a battery, the system

clock will reset to a default date, such as 01/01/2003. In a footnote, Kiper claims that

"although the 'factory default' date could theoretically be any date," he has "never seen one

that is NOT on the first date of the month" of the year of manufacture. I procured a Dell

Dimension 8300-20090330, the same model identified in the folder name, to test Kiper's

claim. As to this model, there were 8 different Basic Input / Output Systems ("BIOS")

software versions released, which were numbered sequentially from A00 to A07. The oldest

was released on 2003-05-06 and the newest was released on 2004-10-01. The third release,

labeled A02, was released on 2003-08-07. I installed the third release on the Dell Dimension

8300, removed the computer's internal battery, and disconnected it from its power outlet.

After reconnecting the power and starting the computer, the computer reverted to its default

date and time of 2003-07-21 00:00:00.

18.   Kiper's report states that with a "bad CMOS battery," a computer "will

continue to reset the system clock to [a default date] every time the computer powers up."

This is misleading, particularly in the case of a Dell Dimension 8300. As long as the

computer is plugged into electronical power, the date and time will continue to progress, and

shutting down or rebooting the operating system will not reset the date. Again, I tested this

using a Dell Dimension 8300. When I removed the internal battery, the clock continued to

progress forward as long as the computer was connected to a power outlet, even while the

computer was turned off. Disconnecting the computer from electricity reset the date to the

default of 2003-07-21. Therefore, a file date of 2003-07-26 could be consistent with using a

Dell Dimension 8300 with a bad battery, running BIOS A02 with a default date of 2003-07-21.

_____
David Loveall II
Senior Computer Scientist
Federal Bureau of Investigation ("FBI")